

Pipes.ai Robocall Mitigation Policy

Last Updated: April 18, 2024

Robocall Mitigation Compliance with TRACED Act

I. Overview

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. Those not yet fully compliant must implement and certify to the implementation of a Robocall Mitigation Plan to ensure that this illegal traffic does not originate on their networks as they work within the industry to become fully compliant. While Pipes.ai takes the position that it does not meet the definition of a voice service provider¹, per DA 24-73 the requirements are more expansive and require additional information from those operating in the industry affected by STIR/SHAKEN. Accordingly, it created this updated Robocall Mitigation Policy.

The Commission requires voice service providers to develop a Robocall Mitigation Plan that:

- details the reasonable steps taken to avoid originating illegal robocalls
- demonstrates a commitment to respond to traceback and FCC requests within 24 hours and to cooperate with investigating and stopping illegal robocalls
- is filed in the Robocall Mitigation Database.

This mitigation plan is submitted on behalf of Pipes.ai (hereinafter “Provider” or “Pipes.ai”). Provider operates a platform that facilitates telecommunications for third party companies (“Clients”) that wish to place prerecorded campaigns and text messaging to communicate with prospective and actual customers. Notably, Pipes.ai obtains DID/Caller IDs that it assigns directly to a particular Client and such Client has no way of changing the DID/Caller ID. Moreover, all numbers will show up in the caller ID through the call or text message and if a consumer calls it back, it is directed back to the Client. This inability to spoof numbers ensures that if Pipes.ai learns of any issues pertaining to a Client campaign, it knows who is responsible and can sever its relationship or direct that any issues be changed. Important to the Pipes.ai platform is that its Clients must include opt-out messaging in any outbound calls and text message.

II. General Prohibition Against Illegal Robocalling

Provider end user services are subject to restrictions contained in its published legal notices and all executed services orders include the requirement that service is provided pursuant to its terms of service (“TOS”) requirements. When Clients engage Pipes.ai, they must agree to comply with all telemarketing and texting laws, including the TCPA and affirm that they have the authority to place prerecorded and/or text messages. This requirement repeats with any new campaign for the same Client. Most recently, with the FCC updating restrictions against opt-ins that allow robocalls on behalf of multiple callers which requirements are to become effective this summer, Provider is in

¹ Pipes.ai is not an actual carrier like a Twilio. Instead, Pipes.ai uses upstream providers like Twilio to purchase DIDs and make phone calls, but Pipes.ai is not, itself a carrier and it does not sell wholesale telco. Instead, Pipes.ai is more of a software company that sits in between an end user brand and a telco provider like Twilio.

the process of requiring all Clients to evidence their opt-ins to show that they are only calling on behalf of a specified entity and not a list of multiple entities.

Pipes.ai's existing TOS prohibit activities normally associated with Robocalling including, but not limited to:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call—again, the platform, itself, ensures that the identity of the sender cannot be altered;
- violating any applicable local, state, or federal law; using the Provider service to engage in or in connection with fraudulent or otherwise unlawful activities.

In addition, the company updated its TOS to expressly require that any Clients notify Pipes.ai if and when it receives a Traceback request. It will respond to Traceback requests if it receives them from a Telecom provider, too. Upon receiving any direct Traceback request, Provider will review its records to determine the Client responsible for a call and immediately contact the Client to obtain information and any necessary support to demonstrate the call was lawful. If the Client does not respond within 18 hours of Provider receiving the original request, Provider will suspend all services, sharing any information it has with the requesting entity regarding the Client that is responsive to the Traceback request.

Discipline/Termination of Clients: Pipes.ai's Clients are notified through their TOS that Pipes.ai may take action up to suspension or termination of service for violation of the TOS. The Clients are expected and required to comply with the TCPA and CTIA's recommendations regarding contacting consumers and if Provider learns that the Client is not abiding by those requirements, depending on the severity of the breach, it may be required to change practices, may temporarily lose its ability to use the platform or may have its services terminated completely. In addition to Pipes.ai restricting its platform to only being able to contact consumer telephone numbers during lawful hours, and not during states of emergency, Pipes.ai's client service team monitors messaging used by its clients on a regular basis to determine if there are any matters of concern that would require additional attention.

III. STIR/SHAKEN Implementation Status

As indicated in the FCC's Robocall Mitigation Database, Pipes.ai's status with respect to STIR/SHAKEN implementation is as follows:

- The Provider has partially implemented the STIR/SHAKEN authentication framework and all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider's service to originate illegal robocalls.
- Since Pipes.ai is not an actual telco carrier and operates in between an end user brand and the telco provider, such providers maintain full STIR/SHAKEN implementations.

IV. Know Your Customer

In order to better prevent or minimize illegal robocall activity, Pipes.ai utilizes the mitigation technique of “Know Your Customer.” The vetting process is intended to help determine the legitimacy of a prospective Client for the purpose of establishing a service relationship. Prior to onboarding a Client, Pipes.ai requires that a contact form and questionnaire be completed. Prospective Clients must provide their taxpayer identification, incorporation details, management team, and other items of identification. Pipes.ai agents then speak with the prospective Client to better understand who they are, where they are located, the types of campaigns they plan to operate, and if they have proper opt-ins or are exempt from consent requirements. Pipes.ai does not work with companies that are located outside of the United States.

Provider efforts to vet retail and business/commercial subscribers occurs during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing the Provider’s required service agreements, and granting the customer the right to use telephone number resources. Commercial end users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers, at Pipes.ai’s discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit.

To further ensure compliance, Pipes.ai requests exemplar opt-ins/marketing and scripting to ensure that the messaging is consistent and that a call recipient would expect the telephone call. Unlike telco providers, Pipes.ai controls the dialing and content within its software. The only calls that can be made through Pipes.ai are within the context of what the company’s software is intended to do and with all the safeguards in place that it built that limit the amount of calls, what time of day the calls can be made, etc. these safeguards prevent unlawful activity.

V. Know Your Upstream Providers

Pipes.ai uses upstream telco providers such as a Twilio or Commio which are nationally recognized and required to have ongoing robocall mitigation policies. Pipe.ai, however, serves as a go-between platform that assists its end user company clients in sending messages or calling specifically opted in telephone numbers.

VI. Traceback and Enforcement Cooperation

Provider commits to respond fully, *within 24 hours*, to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and will actively and timely cooperate with such entities to investigate and stop illegal robocalls using Provider’s services to originate, carry or process illegal robocalls. On a going forward basis, Pipes.ai will include within its services agreements/TOS language requiring Traceback cooperation on any voice service calls exchanged. Such provisions will specify the need for parties to promptly identify upstream providers from which a suspected illegal robocall entered Pipes.ai’s network or the customer of the service from which the call originated.

VII. Ongoing Robocall Mitigation Practices/Call Analytics Systems Used to Identify and Block Illegal Traffic

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns, including complaints from consumers who may assert that they never opted in to being contacted. Since Pipes.ai is not an actual carrier, it does not monitor network usage patterns for consistency with illegal robocalls. However, if it suspects that its customers are using the platform to illegally robocall, it identifies the part and takes appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; terminating the party's ability to communicate through Provider's network/platform; and providing notice to law enforcement authorities.

Since Pipes.ai is not a telco carrier, there is not a call analytics system that would be used to identify or block illegal traffic. Rather, Pipes.ai is able to immediately learn if there are complaints regarding communications stemming from DIDs that it purchases or use of its platform.

VIII. Updates

Pipes.ai will periodically review this Policy and industry practices to see if it can improve its practices to ensure that unlawful robocalls are not placed through its platform. If necessary, it will update this Policy and refile with the FCC.